AMENDMENTS TO THE CLAIMS

Amended claims follow:

1.-12. (Cancelled)

13. (Currently Amended) In an environment that includes a plurality of users, wherein a first user possesses a set of keys, said set of keys including a first key that enables secure communication among a set of users, said set of users including at least said first user and a second user, a keying method, comprising:

[[(a)]]upon eviction of at least said second user, determining an updated first key using information that includes said first key and a second key, wherein said second key enables secure communication among a subgroup of said set of users, wherein said subgroup does not include users subject to said eviction;

wherein said determining uses a function having the following properties: (1) knowledge of said updated first key does not give knowledge of said first key or said second key, (2) knowledge of said first key does not give any knowledge of said updated first key, and (3) knowledge of said first key and said updated first key does not give any knowledge of said second key;

wherein said updated first key is equal to F(first key, second key), wherein F() is a one-way function.

14. (Original) The method of claim 13, wherein only said second user is evicted.

15. (Original) The method of claim 13, wherein said second user and one or more other users in said set of users are evicted.

16. (Cancelled)

17. (Cancelled)

18. (Cancelled)

19. (Original) The method of claim 13, wherein said determining uses only said first key and said second key.

20. (Original) The method of claim 13, wherein said subgroup includes only said first user.

21. (Original) The method of claim 13, wherein said subgroup includes a plurality of users.

22.-40. (Cancelled)

41. (Previously Presented) The method of claim 13, wherein said second key is utilized to update a plurality of compromised first keys by using a one-way function with inputs of said first key and said second key.

42. (Previously Presented) The method of claim 13, wherein said subgroup is a self-repairing group, each member of said subgroup capable of independently updating said first key, where said self-repairing uses a reusable power set, said reusable power set using a power set of said members as a basis for group key updates and including 2^N sets, where N includes the number of said members.

43. (Currently Amended) A key distribution apparatus for use in an environment that includes a plurality of users, wherein a first user possesses a set of keys, said set of keys including a first key that enables secure communication among a set of users, said set of users including at least said first user and a second user, said apparatus comprising:

a key server that determines an updated key upon eviction of at least said second user, using information that includes said first key and a second key, said second key

enabling secure communication among a subgroup of said set of users, wherein said subgroup does not include users subject to said eviction;

said key server using a function having the following properties to determine the updated key: (1) knowledge of said updated first key does not give knowledge of said first key or said second key, (2) knowledge of said first key does not give any knowledge of said updated first key, and (3) knowledge of said first key and said updated first key does not give any knowledge of said second key;

wherein said updated first key is equal to F(first key, second key), wherein F() is a one-way function.

44. (Previously Presented) The apparatus of claim 43, wherein only said second user is evicted.

45. (Previously Presented) The apparatus of claim 43, wherein said second user and one or more other users in said set of users are evicted.

46. (Cancelled)

47. (Cancelled)

48. (Previously Presented) The apparatus of claim 43, wherein said key server uses only said first key and said second key to determine the updated key.

49. (Previously Presented) The apparatus of claim 43, wherein said subgroup includes only said first user.

50. (Previously Presented) The apparatus of claim 43 wherein said subgroup includes a plurality of users.